Dear Reader,

April and May have been very intense! GCSEC joined many international workshops.

On May 14th we joined the 3rd Russian Internet Governance Forum: experts and operators in Russia share the same concerns of many other countries. Minister of Communications proposed to agree on "rules of road" for the Internet, starting from those principles that we all already share. Simple to understand, but complex to achieve, at least considering the very slow progresses on International Cyber Security cooperation.

London Cyber conference, that GCSEC joined in November 2011, started what they called the London process: but without the proper support, we may end up in Bulgaria in fall 2012 talking again about the need of International Cooperation (and we will all agree!).

It is time to act! GCSEC is working with various International organizations (IGF, ITU, OECD, EU) to support the international dialogue and to progress on the definition of basic principles.

On the 16th of May GCSEC gave a speech at the European Parliament thanks to the European Internet Foundation (www.eifonline.org). We raised the awareness of MEPs on the need of a new framework for Digital Identities, including the need for more flexible tools (signature and authentication) that could be easily implemented in EU.

Andrea Rigoni

“Digital inheritance”
by Igor Nai Fovino - PhD – GCSEC
Even if it might seem rather peculiar as last Will, in a digital society as the one in which we live today, similar needs will more and more be common in the near future. According to a survey, 10% of people in the UK insert digital beings in their wills. The study magnified indeed that more than a quarter of people in the UK have hundreds of pounds worth of music and films stored online that they wish to pass on to loved ones.

“How my personal information became bits. A look at Digital Identity management systems” by Marco Caselli – GCSEC
In our daily life we are used to present personal IDs in public offices or banks to access numerous services. This simple gesture makes people sure that we are who we claim to be as well as confirm the personal information we provide. Considering the multiplicity of services that have already migrated into the Internet we are now facing the challenge of virtually sharing this information in the same simple way. Lately, interest on this topic is increasing and the concept of a digital identity (DI), intended as a sort of virtual document, is beginning clearly to take shape.

“Preparing for cyber war... EU-USA joint exercises” - by Maria Luisa Papagni – AlmavivAlGCSEC
The national and international cyber security is one of the main objectives toward which national and international policies tend. It could not be otherwise, since the number of cyber attacks increases and considering that the targets are often Community institutions.
I would like to insert in my Testament my iTunes account, am I crazy?

“Life is beautiful, but, as everything in this world, nothing lasts forever, and soon or later we’ll be obliged to leave all our belongings. I’ve invested thousands of euros in iTunes downloads, and I would like to leave them to my son...am I crazy?”

Even if it might seem rather peculiar as last Will, in a digital society as the one in which we live today, similar needs will more and more be common in the near future. According to a survey by Goldsmiths at the University of London, 10% of people in the UK insert digital beings in their wills. The study, promoted by Rackspace, a cloud computing company, magnified indeed that more than a quarter of people in the UK have hundreds of pounds worth of music and films stored online that they wish to pass on to loved ones.

Inheritance...this is the reason for which everybody should write his Last Will and Testament, to describe how we would like our possessions and assets to be distributed after passing away. The Will is the intention of a testator to legislate. Considering that we spend a huge amount of our life collecting goodwill, fortune and, generally speaking, assets, it is obvious to think that Will generally deal with the concept of property and, more precisely with Movable and Immovable property.

We intend as Immovable property house, estate land, plants, allowances and so on, including also peculiar things as the “right to use an object” or the “right of passage”. In other words, everything attached to the earth fall into this category. Immovable properties had been subject of Will and Testament since the early ages of human society (we can find for example references to Testament and transmission of physical properties in the Roman law).

Things tend to become more complicated with the so-called Movable properties. Traditionally into this class fall cars, furniture, jewels i.e. material things that an executor can re-distribute among the inheritors.

However the class of movable properties is in continuous evolution. Let say for example that in this category at a certain point started to be included Intellectual Property rights, copyrights and everything that is the creation of the human intellect. So, music, literature, discoveries, inventions, phrases etc. started to be considered as something that can and, sometime, must be willed and legated.

This is, indeed, not surprising. Having these intangible properties a not
After that... enjoy your life!

Now making a little step forward, speaking of value, let ask ourselves: has my personal email account a value? Well, lets take me as example: I've started to have an email address 25 years ago. At that time I managed to register my private email account with an email provider that today is very famous and prestigious. Being my surname NAI, my email was a three letters email, nai@xyz.com. Obtaining today a three letters account from this operator (or from other operators) would be almost impossible, moreover, having used as account my family name, I could consider this email address as something I would like my son to inherit.

The value in this case is sentimental, as in the case of a facebook accounts, flickr accounts, Twitter, dropbox etc., but the traditional testaments are indeed full of dispositions with a mere sentimental value, so why do not take into consideration also these aspects when defining a Will?

Things became more evident in situations in which an economical value is involved. Lets consider for example web domains: the trade market of web domains is still appealing, i.e. they can have a remarkable value in term of money. If the owner dies and no one pays the annual fee, they return on the market, causing a loss to the potential inheritors of the original owner.

Making again a little step forward, being the owner of a well-established blog, read by thousand or persons per week, I might have stipulated with some vendors contracts for putting banners on my blog. In that case the blog is actively producing incomes and as in the case of “real companies” I might consider to leave it to my relatives.

The previous examples are, however, only the tip of the iceberg. Paypal accounts, online bank accounts, digital trusts, account balances, online credits, iTunes accounts (again ), digital identities, are what we can define as Digital Inheritance or Digital Estate.

From a legal point of view, even if things might be slightly different in different countries, the tendency is that digital inheritance requires that digital data take part of the descendant's estate. If the digital data are “physically” stored on a media that was in possession of the testator they can be considered directly as movable properties and everything goes smoothly.

The legal and practical problems arise when the testator does not physically possess digital assets, e.g. when the digital asset is stored on a third party server. This is the case for example of cloud-based services. If I physically do not posses an object, how can I leave it as inheritance? Again experience and good sense come in help. In these cases the orientation of the majority of the legislations seems to give an extreme relevance to the concept of password. In other words, if the digital asset, hosted by a service provider, was accessed by the testator using a password, this password will assume the role of the most classic safe box' key, creating possession in a legal sense and falling in this way in the traditional concept of estate.

Even if things might seem simple described in this way, it is indeed true that the matter is still under development and there exist huge differences among the different legislations in the world. A part from the legislative problem, a real obstacle to digital inheritance is that, being so immaterial, to be inherited, the heir should know that the asset exists, and this is not always easy.

So, from a pragmatic point of view, if you would like to leave to your relatives what we called here digital assets, there are only four advices I can give you:

1. Keep track of all your relevant and valuable digital assets, email accounts, paypall accounts, dropbox shares etc.
2. Keep track of the “digital keys” allowing to access to these assets
3. Store and maintain them in a secure digital repository
4. Mention the digital assets in your Will and establish with the help of your lawyer a suitable method for making the digital key-ring available after your departure.

After that... enjoy your life!
“How my personal information became bits. A look at Digital Identity management systems” by Marco Caselli - GCSEC

In our day life we are used to present personal IDs in public offices or banks to access numerous services. This simple gesture makes people sure that we are who we claim to be as well as confirm the personal information we provide. Considering the multiplicity of services that have already migrated into the Internet we are now facing the challenge of virtually sharing this information in the same simple way. Lately, interest on this topic is increasing and the concept of a digital identity (DI), intended as a sort of virtual document, is beginning clearly to take shape.

There is still no common definition but we can basically intend a digital identity as a set of information a user decides to share with an IT system in order to access services on the Web. Seems easy, but nowadays we are forced to deal with lots of DIs at the same time. Let’s think just a second to how many web services we use every day.

Accesses to mail providers, bank accounts, ecommerce portals and social networks are just some of the operations that request a user to login and provide personal information, each time with different rules and security levels. Moreover, a person is usually asked to insert the very same data (name, surname, birth, etc.). This few elements lead us already to a main general issue: is it possible to manage these accounts coherently, securely and avoid the spread of duplicated information?

The current need for a digital identity management system is pushing developers to design secure but usable solutions capable to fill this slice of the IT market.

In the Centralised-Model a DI provider stores all the information and gives data to service providers simply on demand.

In a different manner, within a Federation-Model there is a Provider of Identities that manages the distribution of users’ information among service providers but without storing anything by its own. In this case, the data stays again at service providers’ side but, unlike the Silos-Model, they can be freely used or moved among the federated participants. Lately, a quite different schema called User-Centric is forging consensus among users. In this model, a user is always in control of his/her own information and, formally, he/she stays always in the center of every data transaction. In other words, it will not be possible for any other actor in the system to exchange information without the owner is clearly informed.

There are at least three interesting User-Centric solutions that could become very common and largely used in the near future.

OpenID was probably the first real attempt to take advantage of this logical schema. This infrastructure, designed in 2005, proposes a way to authenticate users in a decentralized manner. The key idea is that a user can freely choose an OpenID provider to store personal information and that the latter assigns to him/her a specific identifier (for example a URL) to access them. Through this identifier the user can use any OpenID-compliant web service demanding authentication and information sharing to the provider and avoiding multiple usernames or passwords. The solution is widely deployed in the Internet but sometimes people complained for a user-friendlier identifier. In fact, linking our identity to a generic URL may sound strange and most recent solutions are trying to eliminate this ambiguity.

This is the case of BrowserID. The solution, proposed by Mozilla, uses in fact email-addresses instead generic identifiers and, compared to OpenID, focuses more on privacy issues. In the previously described OpenID communication protocol DI repositories and web services directly share user’s information. This means that, the firsts know everything a user does with its information. Since this is an obvious privacy concern BrowserID changes radically the way of communicating personal information by demanding more work to the user. The BrowserID authentication process consists on sharing a signed digital certificate where the identity provider asserts that some information really belongs to him/her. This certificate is stored by user’s browser and provided to any BrowserID-compliant web services to perform the login. No other communications are needed and users are ensured to be the only one to keep track of services’ utilization. The idea could be successful but the infrastructure implementation is yet at an embryonic phase.
Cyber Europe 2010
The first exercise, “Cyber Europe 2010”, was conducted November 4, 2010. The main objective was to stimulate and test the cooperation between EU countries in case of attacks on a large scale. Other objectives of this initiative were also to consolidate the trust among member states, to raise awareness about security issues, and sharing around a joint table the cyber-community approach to the issue of cyber security by promoting the exchange of information. About 70 cyber security experts were found to face more than 300 attacks (virtual of course) whose intent was to paralyze the communication between institutions, corporations and private citizens throughout Europe. During the exercise, loss of Internet connection among the countries was simulated. One after the other member states were subjected to increasing problems of access to the network that led to the progressive failure of all links, as shown in figure below:

“Preparing for cyber war... EU-USA joint exercises”
by Maria Luisa Papagni – AlmavivA/GCSEC

The national and international cyber security is one of the main objectives toward which national and international policies tend. It could not be otherwise, since the number of cyber attacks increases and considering that the targets are often Community institutions.

Just think of the repeated fraudulent attacks suffered in the past year by the Emission Trading System (EU ETS) of the European. They caused a cumulative theft of about 2 million permits (more or less equal to 30 million euros) from the national registers of various EU countries, and the subsequent decision of the European Commission to temporarily suspend trading. Besides this example, we must take into consideration also the increasing alarm linked to international terrorism. As direct consequence, the protection of critical information infrastructures (CIIP), became a matter of crucial attention.

“The Commission invites Member States to organise regular exercises for large scale networks security incident response and disaster recovery”. With this communication (1) the European Commission urges to evaluate, and possibly improve, the protection of Critical Information Infrastructures for defending Europe from large scale cyber-attacks and disruptions.

Even during the Ministerial Conference in Tallinn of April 2009 it was highlighted that: “A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission’s action plan”. So, it is perceived that one of the most pressing issues that the cyber community should face is to improve preparedness and response capabilities at national and international attacks or incidents.

In this context arises the work of the European Network and Information Security Agency (ENISA) that, to this end, wants to develop principles and guidelines for Internet resilience, leading pan-European exercises on incidents of large-scale and preparing a framework and a roadmap for European participation in global exercises.
This situation required international cooperation to prevent a total collapse of the virtual network. According to the evaluation report of “Cyber Europe 2010”, multi-level cooperation is necessary to address the threats of global cyber attacks. It is also fundamental the harmonization of standard operating procedures in emergency situations and the definition of the existence of known contact points. The recommendations contained in the document highlight the need to continuously:

- Conduct joint exercises for the protection of critical infrastructure as energy, defense, public administration (according with 86% of participants),
- Have the support and the help of the private sector,
- Ensure a continuous transfer of knowledge and information among participants and
- Determine as soon as a road map to pan-European exercises with scenarios based on more realistic conditions.

Cyber Atlantic 2011

The transatlantic response was the first joint exercise on cyber security between European Union and the United States and held last November 3rd, 2011 focusing on hacking SCADA and Advanced Persistent Threat (APT).

The exercise lasted one day and took the name of Cyber Atlantic 2011. The objectives were mainly to:

- Evaluate the degree of cooperation between the EU Member States and the United States in the management of a cyber-crisis,
- Identify the criticalities of a cyber-crisis management at international level
- Exchange good-practices on how to tackle cyber crisis worldwide.

The exercise involved 20 EU member states, 16 of which with an active role, taking the lessons learned from the first exercise last year’s European Cyber Europe 2010. The exercise began by simulation of crisis scenarios to analyze how the EU and the U.S. would communicate and work collaboratively in case of attacks to their critical infrastructures. In particular, the joint activity between ENISA and the Department of Homeland Security of the United States, has tested two problems that beset the security worldwide: stealing secret information and blocking the productivity of a critical infrastructure of the real world as the energy power generation. The scenarios evoked famous attacks suffered in the same year from Sony Playstation, and the EU Emissions Trading Scheme (described above).

So, in the first scenario was simulated an APT attack, with the theft of sensitive data from the national security agencies of EU countries. The second simulated an attack on the SCADA systems (Supervisory Control and Data Acquisition) of U.S. production facilities used in energy production in Europe. The evaluation report on Cyber Atlantic 2011 has not yet been published.

In the next future...

“Cyber exercises are an important element of a coherent strategy for cyber incident contingency planning and recovery both at the national and European level. […] Such a plan should provide the baseline mechanisms and procedure for communications between Member States and, last but not least, support the scoping and organization of future pan-European exercises. ENISA will work with Member States on the development of such a European cyber incident contingency plan by 2012. In the same timeframe, all Member States should develop regular national contingency plans and response and recovery exercises.” (3)

Member States shall therefore prepare to organize other exercises. The next pan-European exercise on CIIP will be conducted this year. The exercise will be more extensive and sophisticated, which was designed based on experiences and recommendations of the 2010 Cyber Europe.

ENISA considers these exercises a great opportunity to evaluate and especially improve cooperation between the different Member States in the event of a crisis on a large scale. These exercises are also a priority throughout Europe and this need is formulated in the “Digital Agenda for Europe”. Moreover, the first results, as noted above on the report on Cyber Europe 2010, have highlighted the need for more exercises, more cooperation between Member States and the importance of the private sector to ensure information security.

In this context, ENISA will take stock of efforts in the “First International Conference on Cooperation crisis Cyber - Cyber Exercises”. So expect new results for further food for though!

Notes